IET Image Processing

Research Article

IET Journals
The Institution of Engineering and Technology

Controversial 'pixel' prior rule for JPEG adaptive steganography

ISSN 1751-9659
Received on 28th April 2018
Revised 7th September 2018
Accepted on 17th September 2018
E-First on 11th October 2018
doi: 10.1049/iet-ipr.2018.5401
www.ietdl.org

Wenbo Zhou[1], Weixiang Li[1], Kejiang Chen[1], Hang Zhou[1], Weiming Zhang[1] ✉, Nenghai Yu[1]

[1]School of Information Science and Technology, University of Science and Technology of China, Hefei, People's Republic of China

✉ *E-mail: Zhangwm@ustc.edu.cn*

Abstract: Currently, the most successful model for image adaptive steganography is the framework of minimal distortion, in which a reasonable definition of costs can improve the security level. In the authors' previous work, they developed a rule for cost reassignment in spatial domain called the 'controversial pixel prior (CPP)' rule, which defines controversial pixels by utilizing the controversies among several comparable schemes. The CPP rule gives controversial pixels higher modification priorities. In this study, they investigate migrating the CPP rule from the spatial domain to the joint photographic experts group (JPEG) domain and name it the J-CPP rule. In JPEG images, the cover elements are discrete cosine transform (DCT) coefficients and variant factors mayinfluence the distortion definition includingquantisation step, inter-blocks correlation and block energy. However, there is no evidence to reveal which factor is of highest priority for promoting security. In this work, they investigate which factor is more helpful in promoting J-CPP rule, and they finally determine to set the spatial block residual as a penalty to perfect J-CPP rule. Through extensive experiments on different JPEG steganographic algorithms and steganalysis features, they demonstrate that the J-CPP rule can improve the security of JPEG adaptive steganography.

1 Introduction

Steganography is a science and art for convert communication, which aims to hide secret messages into ordinary digital media without drawing suspicion [1–3]. Designing steganographic algorithms for various cover sources [4, 5] is challenging due to the fundamental lack of accurate models. Currently, the most successful approach for designing content-adaptive steganography is based on the framework of minimal distortion, which defines the distortion as the sum of embedding cost between each individual cover element and the corresponding stego object. Syndrome-trellis codes (STCs) [6] provide a general coding method for embedding while minimising an arbitrary additive distortion function with a performance near the theoretical bound.

In modern content-adaptive steganography, the methodology of defining the cost function becomes one of the most important research issues. In the spatial domain, the first method based on the framework of minimal distortion is highly undetectable stego (HUGO) [7]. HUGO defines the pixel's cost as the weighted sum of the difference between feature vectors extracted from a cover image and its stego version in the features of steganalyser subtractive pixel adjacency matrix [8]. However, HUGO can be detected by a steganalyser with a higher dimension of features such as spatial rich models [9], in which the predicted residuals are generated in various directions and manners. In high-dimension features, the correlations between pixels can be further exploited. Therefore, if the pixel can be accurately modelled in any direction, it should be considered a smooth point and assigned a larger cost. With this insight, Holub *et al.* proposed the algorithm wavelet obtained weights (WOW) [10] which assigns high costs to pixels that are more predictable by a bank of directional filters. universal wavelet relative distortion (UNIWARD) [11] generalises the cost function of WOW to make it simpler and more suitable for embedding in an arbitrary domain including the spatial domain and the DCT domain. Li *et al.* [12] proposed the method high-pass, low-pass, and low-pass (HILL), which improves WOW by spreading the costs with a low-pass filter. In HILL [12], the local modification probabilities (MPs) are evened out, and thus the modifications cluster in the complex areas.

As a popular format for image storage and transmission, Joint Photographic Experts Group (JPEG) steganography has become a research hotspot over the past decades. By considering variant influencing factors, several JPEG content-adaptive steganographic algorithms have been proposed. Holub *et al.* developed UNIWARD to the JPEG domain (J-UNIWARD) [13]. Unlike the conventional JPEG steganographic schemes which only embed the secret messages into non-zero AC coefficients, J-UNIWARD uses all DCT coefficients including DCs, zero and non-zero ACs as possible cover elements, and achieves a high level of security performance. However, the high computational complexity of obtaining distortion from the wavelet domain is a major problem. For efficiency, uniform embedding distortion (UED) [14] brings a lightweight distortion metric which merely considers the magnitude of the DCT coefficient in the DCT domain both its intra- and inter-block neighbouring coefficients. Moreover, uniform embedding revisited distortion (UERD) [15] improved UED by exploring the tolerable variation of image statistical model. Hybrid distortion (HDS) [16] exploits block fluctuation via predicting error of pixel in the decompressed image to form a HDS function. Recently, Wei *et al.* [17] proposed an effective definition of distortion function called residual block value (RBV), the method measures block fluctuation by obtaining RBVs of the decompressed image, which can effectively identify complex discernible objects and their orientation.

The above-mentioned methods follow the rule of complexity first and find their way to describe the texture of covers precisely. Note that some of these methods exhibit comparable security performances while defining distortion functions in completely different manners, which demonstrates that they may assign very different costs to the same DCT coefficient. This phenomenon shows the similarity with the spatial domain. In our spatial controversial pixel prior (CPP) rule proposed in [18, 19], we found that several comparable spatial steganographic schemes have similar security performances while defining distortions in very different ways. The costs assigned on some pixels may be large in one method but small in another. We named these pixels Controversial Pixels. The spatial CPP rule works on costs reassignment by giving those controversial pixels higher modification priorities, which are effective for security improvements. Thus, we consider developing the CPP rule from the spatial domain to the JPEG domain. In JPEG steganographic methods, the conception of 'Controversial Pixel' is replaced by

controversial DCT coefficients. These controversial elements are supposed to accommodate more payloads. We name the migrated rule as JPEG controversial 'pixel' prior (J-CPP) rule. Compared to the spatial domain, the JPEG adaptive steganographic methods should be more precise by considering variant important factors such as the quantisation step, intra- and inter-block correlation and the spatial block residual. Thus, we implement a simulation to investigate which factor is more helpful for perfecting the J-CPP rule. We find that the spatial block residual used in RBV is quite helpful to promote the security of J-CPP-based method, thus we use the spatial block residual as a penalty factor to improve the performance of the J-CPP rule.

The rest of this paper is organised as follows. After introducing the framework of minimal-distortion steganography in Section 2, we review the controversial pixel prior (CPP) rule for spatial adaptive steganography in Section 3. In Section 4, we implement a simulation to investigate the most suitable factor for perfecting the form of the J-CPP rule. In Section 5, we provide a full description of the framework of J-CPP-based steganographic scheme and discuss the settings of optimising function. In Section 6, several groups of steganalysis experiments are carried out to verify the advantages of the J-CPP rule. We draw conclusions in Section 7.

2 Preliminaries

In this paper, matrices, vectors and sets are written in boldface, and the k-ary entropy function is denoted $H_k(\pi_1, \ldots, \pi_k)$ for $\sum_{i=1}^{k}\pi_i = 1$.

The cover sequence is denoted as $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, where the signal x_i is an integer such as the quantised value of a DCT coefficient. The embedding operation on x_i is formulated by the range I_i. An embedding operation is called binary if $|I_i| = 2$ and ternary if $|I_i| = 3$ for all i. For example, the ± 1 embedding operation is ternary embedding with $I_i = \{x_i - 1, x_i, x_i + 1\}$.

In the model established in [6], the cover $\boldsymbol{x}$ is assumed to be fixed, so the distortion introduced by changing $\boldsymbol{x}$ to $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ can be simply denoted as $D(\boldsymbol{x}, \boldsymbol{y}) = D(\boldsymbol{y})$. Assume that the embedding algorithm changes $\boldsymbol{x}$ to $\boldsymbol{y} \in \mathscr{Y}$ with probability $\pi(\boldsymbol{y}) = P(Y = \boldsymbol{y})$, which is called the MP, and thus the sender can send up to $H(\pi)$ bits of the message on average with average distortion $E_\pi(D)$ such that

$$H(\pi) = -\sum_{\boldsymbol{y}\in\mathscr{Y}} \pi(\boldsymbol{y})\log \pi(\boldsymbol{y}), \tag{1}$$

$$E_\pi(D) = \sum_{\boldsymbol{y}\in\mathscr{Y}} \pi(\boldsymbol{y})D(\boldsymbol{y}). \tag{2}$$

For a given message length L, the sender wants to minimise the average distortion, which can be formulated as the following optimisation problems:

$$\min_{\pi}\ E_\pi(D), \tag{3}$$

$$\text{subject to } H(\pi) = L. \tag{4}$$

Following the maximum entropy principle, the optimal π has a Gibbs distribution [6]:

$$\pi_\lambda(\boldsymbol{y}) = \frac{1}{Z(\lambda)}\exp(-\lambda D(\boldsymbol{y})), \tag{5}$$

where $Z(\lambda)$ is the normalising factor such that

$$Z(\lambda) = \sum_{\boldsymbol{y}\in\mathscr{Y}} \exp(-\lambda D(\boldsymbol{y})). \tag{6}$$

The scalar parameter $\lambda > 0$ can be determined by the payload constraint (4). In fact, as proven in [20], the entropy in (4) is monotonically decreasing in λ; thus, for a given L in the feasible region, λ can be quickly determined by binary search.

In particular, if the embedding operations on x_i's are mutually independent, the distortion introduced by changing $\boldsymbol{x}$ to $\boldsymbol{y}$ can be considered additive, and is measured by $D(\boldsymbol{y}) = \sum_{i=1}^{n}\rho_i(y_i)$, where $\rho_i(y_i) \in \mathbb{R}^*$ is the cost of changing the ith cover element x_i to y_i ($y_i \in I_i$, $i = 1, 2, \ldots, n$). In this case, the optimal π is given by

$$\pi_i(y_i) = \frac{\exp(-\lambda\rho_i(y_i))}{\sum_{y_i\in I_i}\exp(-\lambda\rho_i(y_i))}, \quad i = 1, 2, \ldots, n. \tag{7}$$

When varying $\lambda \in (0, \infty)$, we can derive a relation between $H(\pi)$ and $E_\pi(D)$, which is called the *rate-distortion bound* [20]. Practical coding methods work under this bound.

In this paper, we consider the case of ternary embedding with the range $I = \{-1, 0, +1\}$, where 0 means that the quantised values of DCT coefficients remain invariant. In general, we assume that

$$\rho_i(-1) = \rho_i(+1) \triangleq \rho_i \in [0, +\infty). \tag{8}$$

Additionally, with (8), it can be assumed that

$$\begin{cases} \pi_i(-1) = \pi_i(+1) \triangleq_i \in \left[0, \frac{1}{3}\right], \\ \pi_i(0) = 1 - 2_i = 1 - p_i. \end{cases} \tag{9}$$

For additive distortion, simulating optimal embedding enables us to test the security of a steganographic method, but once the distortion function is properly defined, we can replace the optimal embedding simulator with off-the-shelf coding methods such as STCs, which can approach the lower rate-distortion bound.

3 CPP rule in the spatial domain

In our previous work [18], an interesting phenomenon was found by comparing different algorithms. Some steganographic methods have similar security performances while defining distortions in very different ways. Moreover, there is a distinction on the cost assignment for some pixels; in other words, the costs assigned on some pixels are large in one method but small in another. We named these pixels 'controversial pixels'. Even with such a discrepancy, several algorithms can still provide the same level of security, which implies that modifications on controversial pixels have little effect on steganalyser. On the basis of this discovery, we proposed CPP rule for cost reassignment in spatial steganography. The CPP rule focuses on those controversial pixels and gives them priority of modification.

As shown in (7), distortions can be converted into MPs, which then determine the payloads assigned on each pixel. Therefore, the CPP rule focuses attention on the MPs when searching for controversial pixels.

Suppose that there are M steganographic methods with comparable security performances, each of them is defined by an additive distortion function D_k for $1 \le k \le M$. The cover is a spatial image consisting of N pixels $\{x_1, \ldots, x_N\}$. For the given payload γ and the distortion function D_k, we calculate the MPs of all N pixels, denoted by $\boldsymbol{p}_k = \{p_{k,1}, p_{k,2}, \ldots, p_{k,N}\}$, $1 \le k \le M$. Collecting all of the probabilities obtained from the M distortion functions, we obtain an $N \times M$ matrix $\boldsymbol{R}$

$$\boldsymbol{R} = [\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_N] = \begin{bmatrix} p_{1,1}, & p_{1,2}, & \cdots, & p_{1,N} \\ p_{2,1}, & p_{2,2}, & \cdots, & p_{2,N} \\ \vdots & \cdots & \vdots & \\ p_{M,1}, & p_{M,2}, & \cdots, & p_{M,N} \end{bmatrix}_{N\times M}$$

Here, the ith column $\boldsymbol{r}_i = \{p_{1,i}, p_{2,i}, p_{3,i}, \ldots, p_{M,i}\}^{\mathrm{T}}$ consists of the MPs of the pixel x_i obtained from the aforementioned M distortion functions. This MP vector records the information of priority for a pixel x_i in different methods. We then compute the statistical

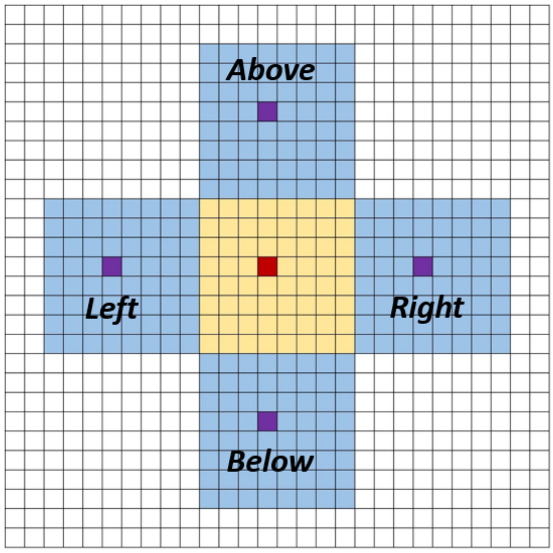

Fig. 1 *Illustration of inter-block correlation*

characteristics of MP vectors to judge the controversial degree of pixels.

To describe the dispersed degree among the elements of $\boldsymbol{r}_i$, we calculate the mean value and second-order centre distance

$$\bar{p}_i = \frac{1}{M}\sum_{k=1}^{M} p_{k,i}, \tag{10}$$

$$v_i = \frac{1}{M}\sum_{k=1}^{M} (p_{k,i} - \bar{p}_i)^2. \tag{11}$$

Here, the second-order centre distance v_i is called the 'probability variance' (PV) of the pixel x_i. With v_i, the degree of controversy is determined. It is obvious that a large v_i reflects that the changing scope of MPs is dramatic, which demonstrates that the priorities of a pixel x_i in different methods are controversial, and this pixel should be given higher modification priority in CPP rule.

For a given payload, the total change rate of pixels is correspondingly determined [21], and too many adjustments may destroy the effectiveness of the original methods. Thus, our proposed CPP rule chooses a certain number of pixels as the controversial pixels. Denote the $(1-\alpha)\%$ quantile of the vector of all PVs: $\boldsymbol{V} = \{v_1, v_2, \ldots, v_N\}$ by T_α; define those pixels with PVs larger than T_α as the controversial pixels, and others are ordinary ones. In other words, the pixels with the top $\alpha\%$ of large PVs are selected as controversial pixels.

Here, the α is called the controversial quantile and T_α is the corresponding controversial threshold. To focus attention only on controversial pixels, we set

$$v_{i'} = \begin{cases} v_i & \text{if } v_i > T_\alpha \\ 0 & \text{otherwise} \end{cases} \quad 1 \le i \le N. \tag{12}$$

In adaptive steganography, the MPs can reflect the priorities of pixels. Thus, the modification priority promotion of controversial pixels can be achieved by increasing their MPs using the following equation:

$$p_i' = \bar{p}_i f(v_i'), \quad 1 \le i \le N, \tag{13}$$

In our past work, the optimising function $f(*)$ has a form of exponential function. Equation (13) can be rewritten as

$$p_i' = \bar{p}_i \mathrm{e}^{v'_i}, \quad 1 \le i \le N. \tag{14}$$

Moreover, the controversial quantile α is simply set proportional relation with payload γ

$$\alpha = 22\gamma. \tag{15}$$

4 Factors influence the migration from CPP to J-CPP

In the spatial domain, the CPP rule deals with the controversial pixels. While in JPEG steganography, we conjecture that the direct migration of CPP by replacing pixels with DCT coefficients may not be efficient because that the compressed format image covers bring many specialities which need to be considered in the J-CPP rule. For instance, UED and UERD consider the intra- and inter-block correlations of DCT coefficients; meanwhile, UERD also defines 'block energy' to help designing distortion function. Some better-security algorithms such as J-UNIWARD and RBV use spatial residual, which precisely reflects the texture of cover images.

In this section, considering the specialities of the JPEG format cover, we list several factors that mainly influence the security of state-of-the-art JPEG adaptive steganography including inter-block correlation, prediction-error-based block energy and spatial block residual. We use different strategies to fuse these factors with the J-CPP rule, the cover elements in J-CPP rule are DCT coefficients, to investigate which factor can help perfect the J-CPP rule executed in the JPEG domain.

(a) Strategy 1: Consider the inter-block correlation

Inter-block correlation reflects the influences caused by neighbouring DCT blocks. It is one of the main differences between the spatial domain and the JPEG domain. For the current DCT coefficient, the cost definition should not only consider the located DCT block but also the adjacent four-neighbourhood blocks.

As shown in Fig. 1, when defining the cost of the red DCT coefficient in the yellow block, the purple DCT coefficients in the blue blocks should be considered. To use the information of inter-block correlation, we make adjustments to the calculation of PV. In the spatial CPP rule, the PVs are calculated by (11) and (12). In this section, we denote the PVs of four purple DCT coefficients in Fig. 1 as $v_{i\mathrm{L}}$, $v_{i\mathrm{R}}$, $v_{i\mathrm{A}}$ and $v_{i\mathrm{B}}$. The PV of the current red DCT coefficient is then recalculated

$$u_i = v_i + v_{i\mathrm{L}} + v_{i\mathrm{R}} + v_{i\mathrm{A}} + v_{i\mathrm{B}}, \tag{16}$$

$$v_{i'} = \begin{cases} u_i & \text{if } u_i > T_\alpha \\ 0 & \text{otherwise} \end{cases} 1 \le i \le N. \tag{17}$$

where v_i' is the PV of the selected controversial element and contains the information of inter-block correlation and T_α is the controversial threshold same as it in (12).

(b) Strategy 2: Use prediction-error-based block energy as a penalty

Block energy is used to design distortion function in UERD and HDS. The definitions of block energy of these two methods are quite different. In UERD, the block energy is defined as the sum of DCT coefficient value multiplying its quantisation step. While in HDS, the block energy is defined as the sum of spatial block prediction errors. The prediction errors of spatial pixels precisely reflect the texture of the image, which results in better security for HDS than UERD. Thus, we take the prediction-error-based block energy as another affecting factor.

Denote $E_{m,n}$ as the block energy of the (m, n)th 8×8 DCT block. The $E_{m,n}$ is defined as the sum of spatial block prediction errors

$$E_{m,n} = \sum_{i=1}^{64} e_i. \tag{18}$$

where e_i is the prediction error of the spatial pixel, which corresponds to the current DCT coefficient.

We utilise the prediction-error-based block energy by multiplying $E_{m,n}$ as a penalty to PV

$$u_i = \begin{cases} v_i & \text{if } v_i > T_\alpha \\ 0 & \text{otherwise} \end{cases} \quad 1 \le i \le N. \tag{19}$$

$$v_i' = u_i \times E_{m,n}, \tag{20}$$

By (20), the controversial elements' PVs obtain promotion according to the texture of their located block.

(c) Strategy 3: Use spatial block residual as a penalty

This strategy is somewhat similar to strategy 2. Both of the spatial block residuals and the prediction errors can reflect the texture of the current image block. The spatial residual is obtained by predicting the pixel with a bank of directional filters and describes the texture of image more precise than the prediction error, which is only calculated by surrounding pixels in a first-order form. For simplicity, we denote the spatial block residual value of the (m, n)th DCT block as $B_{m,n}$. Similar to strategy 2, we use $B_{m,n}$ as a penalty multiplied with PV

$$u_i = \begin{cases} v_i & \text{if } v_i > T_\alpha \\ 0 & \text{otherwise} \end{cases} \quad 1 \le i \le N. \tag{21}$$

$$v_i' = v_i \times B_{m,n}, \tag{22}$$

By comparing strategy 2 and strategy 3, we can investigate that whether more precise spatial information leads to better security.

All these factors may influence the migration from CPP to J-CPP. To investigate the effect brought by different factors, we implement a simulation with the following steps:

(a) Randomly select 1000 grey-scale images of size 512 × 512 from the BOSSBase ver.1.01 database [22], then the 1000 images are compressed into JPEG domain with a quality factor (QF) = 75.
(b) Choose two comparable JPEG steganographic methods UERD and HDS as basic methods to apply J-CPP rule. Use original J-CPP rule [v_i' calculated by (12)] and adjusted J-CPP rule combined with factor 1 to factor 3 [v_i' calculated by (17), (20) and (22), respectively) to define the distortions of covers. For simplicity, the direct migrated J-CPP (UERD, HDS) and the adjusted J-CPP rule fused with factor 1 to factor 3 are denoted J-CPP(S0), J-CPP(S1), J-CPP(S2) and J-CPP(S3), respectively.
(c) Generate stegos corresponding to the methods in step (b) under the payload of 0.3 bpnzAC (bit per non-zero AC coefficient). Then, extract the 8000-D discrete cosine transformation residual (DCTR) [23] steganalytic feature vector from cover images and each stego object.
(d) Calculate the maximum mean discrepancy (MMD) [2], which measures the distance between the feature set of cover images and that of stego images, (smaller MMD means better security) between each pair of the cover feature vector and stego feature vector. Obtain the average value of the MMD and standard deviation over ten different independent tests on the dataset, and then make a comparison.

From the statistical results of Table 1, we can observe the security performances of different embedding strategies. The MMD obtained by original J-CPP is close the HDS, which verifies our conjecture that the direct migration of CPP from spatial domain has little effect on the security. While combining with different influencing factors, the J-CPP receives various degrees of promotion. Specifically, the promotion brought by *strategy 3* is more than that of *strategy 2*, which indicates that the spatial block residual value $B_{m,n}$ is a better penalty than the prediction-error-based block energy $E_{m,n}$.

Table 1 Simulation results of MMD and corresponding standard deviation

Payload	Embedding method	MMD
0.3 bpnzAC	UERD	$3.6745 \times 10^{-6} \pm 0.0042$
	HDS	$3.1217 \times 10^{-6} \pm 0.0045$
	J-CPP(S0)	$3.1010 \times 10^{-6} \pm 0.0036$
	J-CPP(S1)	$3.0441 \times 10^{-6} \pm 0.0038$
	J-CPP(S2)	$2.9757 \times 10^{-6} \pm 0.0038$
	J-CPP(S3)	$2.8288 \times 10^{-6} \pm 0.0041$
	J-CPP(S1,S2,S3)	$2.9822 \times 10^{-6} \pm 0.0037$

The simulation results demonstrate that considering influencing factors of JPEG's specialities can help promote the security level of J-CPP rule. Thus, we utilise the spatial block residual value $B_{m,n}$ as a penalty, which shows better effectiveness to perfect our J-CPP rule in the next section.

5 J-CPP rule

In this section, we make a full description of the J-CPP-based steganographic algorithm. We utilise the spatial block residual value as a penalty to adjust the optimising function in (13). The bottom half of this section is a discussion of some important issues of J-CPP rule.

5.1 Description of the J-CPP-based algorithm

Similar to the spatial domain, the J-CPP rule is used based on several JPEG steganographic methods with comparable security performances. In J-CPP rule, the controversial pixels are replaced by controversial DCT coefficients.

Following the definition of spatial CPP rule, we start from the modification probabilities of DCT coefficients. For a given payload γ and several basic distortion functions D_k $(1 \le k \le M)$, we obtain an MP vector of DCT coefficient x_i, denoted $\boldsymbol{p}_i = \{p_{1,i}, p_{2,i}, \ldots, p_{M,i}\}$, $1 \le i \le N$. We then compute the second-order centre distance v_i of the MP vector $\boldsymbol{p}_i$ to judge the controversial degree. Set α as controversial quantile, and T_α is the corresponding controversial threshold. Then, the controversial DCT coefficients are selected by (21) and the PVs' set of controversial DCT coefficients is $\{v_{i'}\}$ (here $v_{i'}$ is equivalent to the u_i in (21).

Assume the DCT coefficient x_i is located in the (m, n)th DCT block of cover image ($1 \le m \le a$ and $1 \le n \le b$, where $a \times b$ is the total amount of image blocks), the spatial block residual of the current block is denoted as $B_{m,n}$. Here, $B_{m,n}$ should be scale normalised first. Since that the huge discrepancy of scale in $\boldsymbol{B} = \{B_{m,n}\}$ may cause disadvantages to the J-CPP rule. We set

$$\boldsymbol{B}' = \frac{\boldsymbol{B}}{\max\{\boldsymbol{B}\}}. \tag{23}$$

thus we have $\max\{\boldsymbol{B}'\} = 1$.

In the next section, we will search for the best strategy to utilise the scale-normalised $B'_{m,n}$. A larger $B_{m,n}$ represents the more textured cover block, and the controversial DCT coefficients in these more textured blocks should be allocated higher modification priority. Considering $B'_{m,n}$ as a penalty, we determine the MP adjustment function as the following form of the composite function:

$$p_{i'} = \bar{p}_i f(\omega(B'_{m,n}, v'_i))(), \quad 1 \le i \le N. \tag{24}$$

where $\bar{p}_i$ is calculated by (10), $f(*)$ and $\omega(*)$ are optimising function and penalty function, respectively.

We suppose the optimising function $f(*)$ has the following two important attributes:

(i) The value domain of $f(*)$ should theoretically be $[1, +\infty)$, and $f(0) = 1$, because the modification priority of controversial DCT coefficient is supposed to be promoted, thus the adjusted MP p_i' should never be smaller than the original $\bar{p}_i$. The function $f(*)$ should be no smaller than 1.
(ii) The optimising function $f(*)$ should be monotonically increasing, which based on the assumption that the more controversial DCT coefficients are, the higher priorities they have.

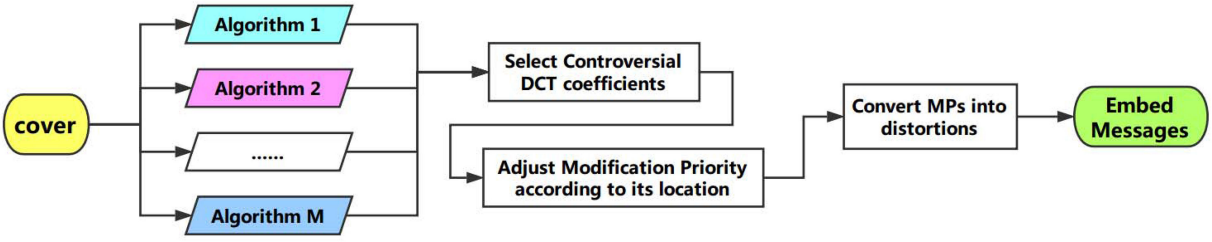

Fig. 2 *Flowchart of the J-CPP rule-based algorithm*

Table 2 MMD values corresponding to different t

Values of t	0.10	0.15	0.20	0.21
MMD (10^{-6})	3.1097	3.0296	3.0106	2.9480
values of t	0.22	0.23	0.25	0.30
MMD (10^{-6})	2.7534	2.9681	3.204	3.3645

The controversial DCT coefficient's priority can be sufficiently promoted when its v_i' value is sufficiently large.

Following the investigation in our previous work [18], we adopt an exponential form for $f(*)$. In addition, due to the direct correlation between the spatial block residual value matrix $\boldsymbol{B}$ and the image texture, we define the $\omega(*)$ with a linear relation between $B'_{m,n}$ and v_i'. Then, the MP adjustment function is finally written as

$$p_i' = \tilde{p}_i \mathrm{e}^{k B'_{m,n} v'_i}, \tag{25}$$

where k is a proportionality coefficient and $1 \le i \le N$, $1 \le m \le a$, $1 \le n \le b$.

Note that, for ± 1 embedding, when $p_i = 2/3$, the DCT coefficient x_i has the largest average payload, $\log_2 3$ (which is consistent with the assumption in (9)). Therefore, we limit the adjusted MPs by

$$p_i'' = \min\left\{p'_i, \frac{2}{3}\right\}, \quad 1 \le i \le N. \tag{26}$$

Actually, p_i'' is not the final MP that we used for embedding. Since that after the adjustments by (25) and (26), the total information entropy is no more under the constraint of original payload. Therefore, we should flip the MP to distortion and then use the practical off-the-shelf coding methods STCs.

Denoting $\pi_i(+1) = \pi_i(-1) = p_i''/2$ and $\pi_i(0) = 1 - p_i''$, by (7), the corresponding distortion function $\rho_i(l)$ $(l \in I)$ satisfies

$$\pi_i(l) = \frac{\exp(-\lambda\rho_i(l))}{\sum_{l \in I}\exp(-\lambda\rho_i(t))}, \quad l \in I; \quad 1 \le i \le N. \tag{27}$$

To solve $\rho_i(l)$ from (27), without loss of generality, we can set $\lambda = 1$ because λ is monotonically decreasing with respect to the message length as proven in [20]. Moreover, the transformed distortion has the form

$$\rho_i(l) = \ln\frac{\pi_i(0)}{\pi_i(l)}, \quad l \in I, \quad 1 \le i \le N. \tag{28}$$

We call $\rho_i(l)$ in (28) the adjusted distortion function, it can be easily verified that the adjusted distortion satisfies (27).

Eventually, we obtain a new steganographic algorithm determined by the adjusted distortion function (28), according to which we embed messages under the payload of γ by using STCs. The framework of J-CPP rule is depicted in Fig. 2 and the details of the J-CPP-based method are described in Algorithm 1.

Algorithm 1: J-CPP-based algorithm

Input: A cover image $\boldsymbol{x}$ with N DCT coefficients $x_1, \ldots, x_N$; payload γ; M comparable JPEG distortion functions; k.

Output: The stego image $\boldsymbol{y}$.

1. Set a controversial threshold T_α according to the given payload γ, and input the optimal proportionality coefficient k.
2. Compute MP vector $\boldsymbol{p}_i = \{p_{1,i}, p_{2,i}, \ldots, p_{M,i}\}$ $(1 \le i \le N)$ of all x_i using the M distortion functions, according to the payload γ.
3. Calculate the PV v_i for x_i, determine whether it is a controversial DCT coefficient, and calculate the $B_{m,n}$ for the current block.
4. Use $B_{m,n}$ as a penalty, adjust the controversial DCT coefficients' MPs with (25) and (26), and then convert them into adjusted distortion functions with (28).
5. Embed messages into cover image $\boldsymbol{x}$. Implement STCs under the payload of γ according to the adjusted distortions, and finally output the stego image $\boldsymbol{y}$.

5.2 Determinations of α and k

In spatial steganographic algorithms, the modification is directly added on single spatial pixel and not spread to others. While in the JPEG domain, the change on one DCT coefficient reflects on a wide range of spatial pixels because of the DCT transformation. Too many adjustments on the DCT coefficients may be counterproductive. Thus, the choice of priority-promoted DCT coefficients should be considered carefully.

The purpose of the J-CPP rule is to promote the modification priorities of the controversial DCT coefficients, which can be achieved by (25). There are two important parameters in J-CPP rule, controversial quantile α and proportionality coefficient k, which determine the amount and location of controversial DCT coefficients. In this section, we discuss the optimal choices of α and k.

(a). Investigation on α

We first consider the controversial quantile α. Without loss of generality, we set $k B'_{m,n} = 1$ in (25) to focus attention on v_i. In [21], Li *et al.* proved that the cover elements change rate R_c has a linear relation with payload γ, and the relation is also established in the JPEG domain. In our previous work [18], we verified that in spatial CPP, the optimal α has a linear relation with R_c, and can be simplified as a proportionality with γ as (15). Here, we follow the form of (15) and set $\alpha = t\gamma$ in J-CPP. We search the most suitable proportional coefficient through a group of experiments.

We use the database BOSSbase ver.1.01 [22] to search for the optimal value of t, and BOWS-2-OrigEP3 [24] (simplified as BOWS2) for verification. About 1000 grey-scale images are selected from BOSSbase database to calculate MMDs and the whole BOWS2 is used for steganalysis. The covers used are compressed into JPEG domain with QF QF = 75. UERD and HDS are two basic algorithms used in J-CPP rule [denoted J-CPP(UERD, HDS)], the steganalytic feature is DCTR. We first calculate the MMDs under 0.3 bpnzAC between cover set and its stego object with varying values of t. We list the results in Table 2 and plot the curve of MMDs with respect to t in Fig. 3*a*.

Coincidentally, the optimal t is 0.22, which is consistent with it in spatial CPP rule. To verify the optimal t is not an overfitted parameter to cover set, we make a test by steganalysis on BOWS2. The testing error curve in Fig. 3*b* indicates that 0.22 is also the optimal parameter for other databases. In summary, we set

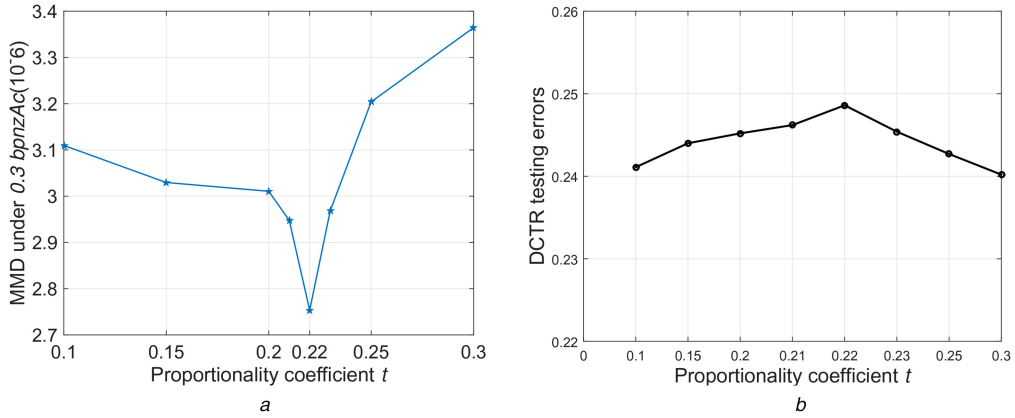

Fig. 3 *Varying trends of security level with respect to (w.r.t.) proportionality coefficient t*
(a) MMDs based on BOSSbase, ***(b)*** DCTR testing errors based on BOWS2

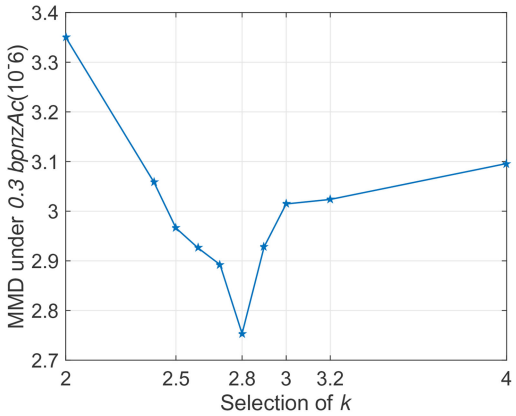

Fig. 4 *Varying trends of security level w.r.t. proportionality coefficient k*

$\alpha = 0.22\gamma$ in J-CPP rule. With the help of α, we can easily locate the controversial DCT coefficient under different payloads.

(b). Analysis of k

Another issue is the choice of k for (25). In J-CPP rule, the controversial DCT coefficients are limited to a certain number. Some of them are located in textured blocks, and others are in smooth blocks. As mentioned above, the purpose of using $\boldsymbol{B}$ in the J-CPP rule is to ensure the priority-promoted DCT coefficients located in textured blocks. Thus, we can control the degree of priority promotion for controversial elements through selecting a suitable k.

Comparing to the original J-CPP rule [which has the form of (14)], the new modification priorities of controversial DCT coefficients located in textured blocks should be much higher, which means higher MPs. Denoting the MPs calculated by (25) and (14) are p_{A} and p_{B} respectively. Thus, we have $p_{\mathrm{A}} > p_{\mathrm{B}}$. Under this condition, we can theoretically analyse the lower bound of k as follows:

$$\begin{aligned} p_{\mathrm{A}} > p_{\mathrm{B}} &\Rightarrow \frac{p_{\mathrm{A}}}{p_{\mathrm{B}}} > 1 \\ &\Rightarrow \frac{\mathrm{e}^{kB_\alpha v_i}}{\mathrm{e}^{v_i}} > 1 \Rightarrow \mathrm{e}^{(kB_\alpha - 1)v_i} > 1 \\ &\Rightarrow kB_\alpha - 1 > 0 \Rightarrow k > \frac{1}{B_\alpha} \end{aligned} \tag{29}$$

Here, B_α is a selected threshold for all $B'_{m,n}$. In analogy with the controversial threshold T_α, if $B'_{m,n} > B_\alpha$, the current block at (m, n) is considered textured; otherwise, the current block is not textured. We use α as the quantile for $\boldsymbol{B}$ as well, and thus, the number of DCT coefficients located in textured blocks would be no less than those controversial ones. In addition, the modification priorities of controversial elements located in textured blocks can get a further promotion ($kB > 1$; thus, $\mathrm{e}^{(kB-1)v_i} > 1$ and $p_{\mathrm{A}} > p_{\mathrm{B}}$), while those in smooth blocks are correspondingly reduced or keep constant ($kB \leqslant 1$, $p_{\mathrm{A}} \leqslant p_{\mathrm{B}}$).

Table 3 Statistics on the number of different DCT coefficients

Classification	Percentage in the cover, %
controversial DCT coefficients (N_1)	6.5918
coefficients in textured blocks (N_2)	6.5998
controversial coefficients in textured blocks (N_3)	1.7078
N_3/N_1	25.88

In practise, the texture of each cover image is different. To set a reasonable B_α for all databases, we mix the BOSSbase and BOWS2. We then randomly select 1000 images from 5000 most textured images of the mixed database to calculate B_α. Finally, the average value B_α is obtained as 0.3947. With (29), the searching range of optimal k is shrunk, and the lower bound of k is 2.52.

The lower bound identifies us a probable range for searching optimal k, based on which we executed a group of experiments. We calculate the MMDs of J-CPP(UERD, HDS) with varying values of k under 0.3 bpnzAC. The used cover set contains 1000 images of BOSSbase with QF = 75. In addition, the steganalytic feature is DCTR. We plot the curve of MMDs with respect to k in Fig. 4.

The results in Fig. 4 are accorded with our inference on k and the curve of security performance has a local optimum. Thus, we fix $k = 2.8$ in our J-CPP rule.

As mentioned above, the modification priorities of different controversial elements are readjusted according to their location. Some of them are further promoted and others are correspondingly reduced. We use 1013.jpg from the BOSSbase with QF = 75 as an example and make a statistic on the numbers of different kinds of DCT coefficients in Table 3, the payload is 0.3 bpnzAC.

Here, N_1 is the number of controversial DCT coefficients selected with α, N_2 represents the total coefficients of textured blocks and N_3 is the number of controversial DCT coefficients located in textured blocks. The statistical results show that N_2 is larger than N_1, which conforms to our expectation. N_3 is only one-quarter of N_1, which indicates that the number of further priority-promoted coefficients is only a small part. The modification on these coefficients will not influence the spatial pixels, which is also expected.

6 Experiments

6.1 Setups

In this paper, the BOSSbase ver.1.01 database [22], which contains 10,000 512×512 8 bit grey-scale images, is used as the image database. All of the images are compressed into JPEG domain with QF = 75 and 95. We replace STCs with an optimal embedding

simulator [25] for executing embedding according to distortions, which can reach the theoretically optimal bounds of security. All algorithms are tested under the payload range from 0.1 to 0.5 bpnzAC (bit per non-zero AC coefficient). The detector is trained by two state-of-the-art steganalytic features, 8000-D DCTR [23] and 17000-D representation using Gabor filter (GFR) [26] with ensemble classifiers [27]. The ensemble by default minimises the total classification error probability under equal priors $P_E = \min_{P_{FA}} (1/2)(P_{FA} + P_{MD})$, where P_{FA} and P_{MD} are the false-alarm probability and the missed-detection probability, respectively. The ultimate security is qualified by average error rate $\bar{P}_E$ averaged over ten 5000/5000 database splits, and larger P_E means stronger security.

6.2 Selection of basic steganographic methods for the J-CPP rule

As verified in spatial CPP rule, any pair of steganographic methods can be used as basic seed functions as long as they have similar security performances, and the number of basic methods can be three or more. In J-CPP rule, we also select those methods with comparable security level as seed methods. Some off-the-shelf methods can be used as examples to verify the effectiveness of J-CPP rule.

When QF = 75, UERD and HDS are the first pair in our experiments. The security performances under the detection of DCTR of these two methods are extremely close to each other. Moreover, HDS performs slightly better than UERD for some payloads under the detection of GFR. The J-CPP rule based on UERD and HDS is denoted as J-CPP(UERD, HDS).

RBV and J-UNIWARD comprise another pair of examples in the following experiments. Both of these two algorithms use the information of spatial residuals to define distortion function. The difference is that RBV defines costs directly on DCT coefficients by considering the intra- and inter-block spatial residual values, while the costs in J-UNIWARD is computed as a sum of relative changes of coefficients in a directional filter bank decomposition of the decompressed cover image. When QF = 75, RBV achieves higher security level than J-UNIWARD for some payloads under the detections of DCTR and GFR. We use this pair for verification, denoted J-CPP(RBV, UNI).

We also use another pair consisting of UERD and J-UNIWARD as examples when QF = 75. The forms of these two steganographic algorithms are totally different, and J-UNIWARD outperforms UERD from the payloads of 0.1–0.5 bpnzAC (J-UNIWARD also has a high computational complexity) under the detection of DCTR and GFR. This pair, denoted J-CPP(UERD, UNI), is used to investigate that whether J-CPP rule is still effective when the form and security level of basic methods are different.

With regard to QF = 95, the quality of the compressed image is better than QF = 75. Moreover, the overall security level of steganography is improved. The discrepancy among different algorithms is also changed. HDS outperforms quite better than UERD under the detection of DCTR and GFR, and the security performances of RBV and J-UNIWARD become closer to each other. Although the situation changed, we still use (UERD, HDS) and (RBV, UNI) as two examples in our experiments to demonstrate that our J-CPP rule is always effective.

6.3 Comparison of security levels

In this section, we conduct several steganalysis experiments to verify that our proposed J-CPP-based scheme outperforms seed methods. The first part of our experiments is executed on the compressed JPEG covers with QF = 75. The first pair of examples for the J-CPP is J-CPP(UERD, HDS). The second group of experiments is to test the security level of J-CPP(RBV, UNI). For intuition, we use histograms to compare the testing errors of these two groups of methods in Fig. 5.

The third pair of examples to verify the effectiveness of J-CPP is J-CPP(UERD, UNI). The security levels of the two methods are close and the differences between their testing errors are similar to that of RBV and J-UNIWARD. This group of experiments is used to detect whether the J-CPP rule is limited by the form of seed distortion functions. The comparison is depicted in Fig. 6. The numerical values of testing errors and standard deviations for QF = 75 are listed in Table 4. The promotion is calculated as the difference in security performances between J-CPP-based methods and one of its better seed methods.

The second part of our experiments is executed on the compressed JPEG covers with QF = 95. We use two pairs of examples, J-CPP(UERD, HDS) and J-CPP(RBV, UNI), to verify that the J-CPP rule still works when the QF is higher. The comparison results are shown in Fig. 7. In addition, the numerical values of testing errors and standard deviations for QF = 95 are listed in Table 5.

In Figs. 5*a* and *b*, J-CPP(UERD, HDS) always has a higher level of security than UERD and HDS under the detection of DCTR and GFR for various payloads when QF = 75. The security performance is improved at most 1.45% against DCTR and 1.40% against GFR. In Figs. 5*c* and *d*, the J-CPP-based scheme also improves the level of security for RBV and J-UNIWARD under DCTR and GFR. It is worth mentioning that the promotion in Fig. 5*d* against GFR is not as conspicuous as it in Fig. 5*c* against DCTR. RBV has a more significant promotion than J-UNIWARD under the detection of GFR when QF = 75 which means that the security performances of RBV and J-UNIWARD are not that comparable. This divergence probably causes a negative influence on J-CPP rule.

In Fig. 6, the J-CPP rule scheme also shows an improved level of security by combining UERD and J-UNIWARD under DCTR and GFR. The improvements are conspicuous and can reach 1.94% against DCTR when the payload is 0.4 bpnzAC and 2.10% against GFR under 0.4 bpnzAC. The results demonstrate that the J-CPP rule is not limited to the components of its basic methods. Theoretically, any different type of adaptive steganography can be used as the basic method of our J-CPP rule.

When QF = 95, the quality of the cover images is much better than QF = 75, and the overall security level of steganography has a significant improvement. The room for improvement is limited due to the high level of current security performances. However, we can still use J-CPP rule for a further promotion in security performance. Moreover, the improvement in J-CPP(RBV, UNI) against DCTR can even reach a high level of 2.30%.

The improvements of J-CPP rule are statistically significant. The statistical significance can be verified by a hypothesis testing called ‘ 5×2-fold cross-validated paired t test’, which has been used in Section 6.4 of our previous work [18]. The improvements which are statistically significant under a significance level of 0.05 are bold and underlined in Tables 4 and 5.

7 Conclusion

Currently, the minimal-distortion-based steganography has been proven the most effective model for adaptive steganography. In this paper, we extend our previous work, CPP rule in the spatial domain, to JPEG domain as J-CPP rule. This rule aims to improve the security performances of JPEG steganography by fusing several comparable algorithms. The experiments show that the J-CPP rule can improve the security of the state-of-the-art steganographic algorithms.

The J-CPP rule considers a combination of several off-the-shelf methods instead of remaining focusing attention on a single method. J-CPP rule is amended according to the specialities of JPEG image. The effectiveness of J-CPP rule is not limited to the forms of basic methods. Moreover, if the selected candidate algorithms for J-CPP rule have comparable security performances, the improvement of security can reach a higher level. In addition, the J-CPP rule provides a novel tool for designing steganographic schemes as spatial CPP. There is no need to struggle in designing a new method outperforming previous ones. It makes sense if the proposed method is comparable with previous ones, and then we can promote it with the help of J-CPP rule.

In the present paper, we migrate the spatial CPP rule to the J-CPP rule in the JPEG domain. In our future work, fusing more

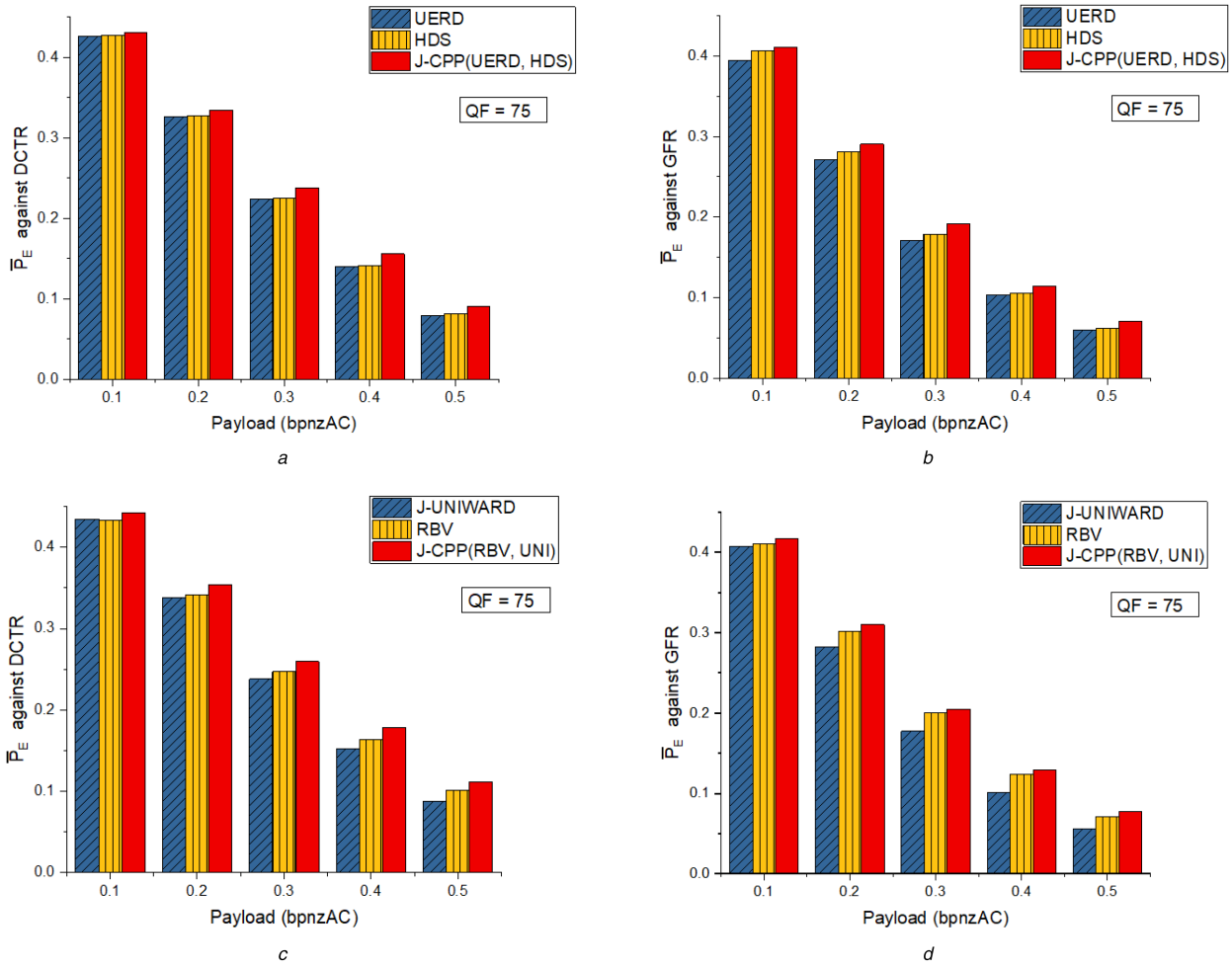

Fig. 5 *Testing errors under the detection of two steganalysis features with QF = 75*
(a) UERD, HDS and J-CPP (UERD, HDS) against DCTR, ***(b)*** UERD, HDS and J-CPP (UERD, HDS) against GFR. ***(c)*** J-UNIWARD, RBV and J-CPP (RBV, UNI) against DCTR, ***(d)*** J-UNIWARD, RBV and J-CPP (RBV, UNI) against GFR

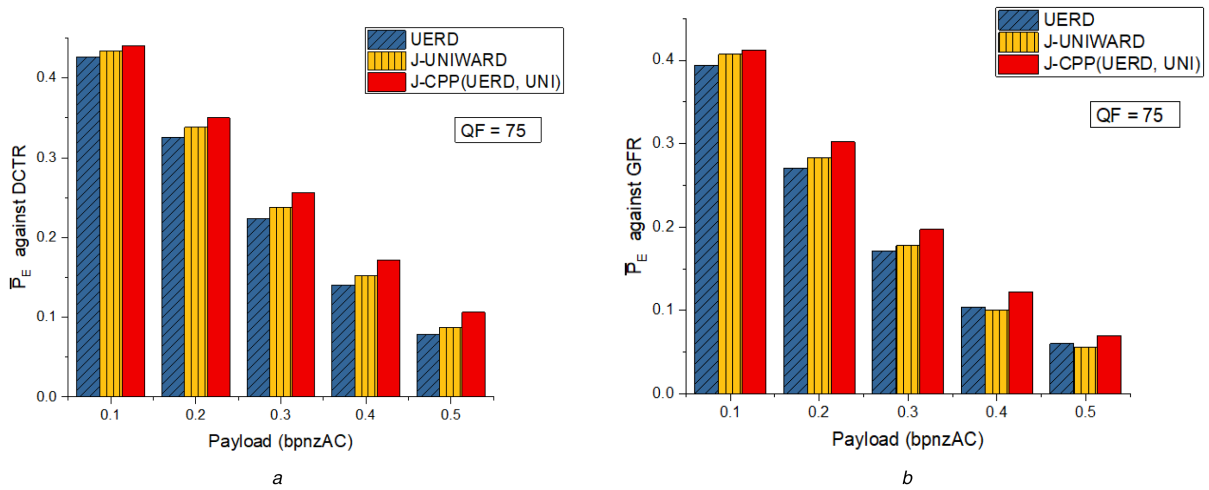

Fig. 6 *Testing errors for UERD, J-UNIWARD and J-CPP (UERD, UNI) under the detection of two steganalysis features with QF = 75*
(a) DCTR, ***(b)*** GFR

basic methods in the J-CPP rule and developing a framework of evolutionary steganography is an interesting direction, which can be achieved by iteratively executing the J-CPP rule.

8 Acknowledgment

This work was supported in part by the Natural Science Foundation of China under Grant nos. U1636201 and 61572452.

Table 4 Numerical values of testing error and standard deviation for Figs. 5 and 6

Feature	Embedding method	Testing errors from 0.1 to 0.5 bpnzAC				
		0.1	0.2	0.3	0.4	0.5
DCTR	UERD	0.4264 ± 0.0023	0.3259 ± 0.0024	0.2242 ± 0.0021	0.1401 ± 0.0011	0.0789 ± 0.0013
	HDS	0.4276 ± 0.0018	0.3275 ± 0.0028	0.2247 ± 0.0022	0.1410 ± 0.0015	0.0814 ± 0.0019
	J-CPP(UERD,HDS)	0.4306 ± 0.0021	0.3347 ± 0.0025	0.2383 ± 0.0023	0.1555 ± 0.0013	0.0901 ± 0.0013
	promotion, %	0.3	**0.72**	**1.36**	**1.45**	**0.87**
	RBV	0.4328 ± 0.0031	0.3414 ± 0.0026	0.2471 ± 0.0028	0.1640 ± 0.0017	0.1012 ± 0.0018
	J-UNIWARD	0.4344 ± 0.0014	0.3382 ± 0.0022	0.2379 ± 0.0017	0.1525 ± 0.0026	0.0873 ± 0.0015
	J-CPP(RBV, UNI)	0.4424 ± 0.0018	0.3538 ± 0.0019	0.2595 ± 0.0013	0.1780 ± 0.0015	0.1115 ± 0.0014
	promotion, %	**0.8**	**1.24**	**1.24**	**1.40**	**1.03**
	J-CPP(UERD, UNI)	0.4399 ± 0.0030	0.3501 ± 0.0013	0.2566 ± 0.0018	0.1719 ± 0.0018	0.1064 ± 0.0015
	promotion, %	0.55	**1.19**	**1.87**	**1.94**	**1.91**
GFR	UERD	0.3944 ± 0.0029	0.2708 ± 0.0023	0.1714 ± 0.0013	0.1036 ± 0.0011	0.0602 ± 0.0008
	HDS	0.4059 ± 0.0031	0.2814 ± 0.0028	0.1788 ± 0.0020	0.1058 ± 0.0014	0.0616 ± 0.0010
	J-CPP(UERD, HDS)	0.4103 ± 0.0039	0.2903 ± 0.0022	0.1917 ± 0.0025	0.1143 ± 0.0016	0.0702 ± 0.0007
	promotion, %	0.44	**0.89**	**1.29**	**0.85**	**0.86**
	RBV	0.4111 ± 0.0021	0.3020 ± 0.0027	0.1999 ± 0.0024	0.1243 ± 0.0023	0.0710 ± 0.0018
	J-UNIWARD	0.4072 ± 0.0024	0.2826 ± 0.0014	0.1777 ± 0.0018	0.1010 ± 0.0018	0.0564 ± 0.0009
	J-CPP(RBV, UNI)	0.4173 ± 0.0029	0.3101 ± 0.0021	0.2052 ± 0.0024	0.1294 ± 0.0011	0.0775 ± 0.0007
	promotion, %	0.62	**0.81**	0.53	**0.51**	**0.65**
	J-CPP(UERD,UNI)	0.4122 ± 0.0023	0.3022 ± 0.0031	0.1973 ± 0.0024	0.1220 ± 0.0017	0.0699 ± 0.0016
	promotion, %	0.50	**1.96**	**1.96**	**2.10**	**0.97**

Bold values indicate the statistical significance of the promotion.

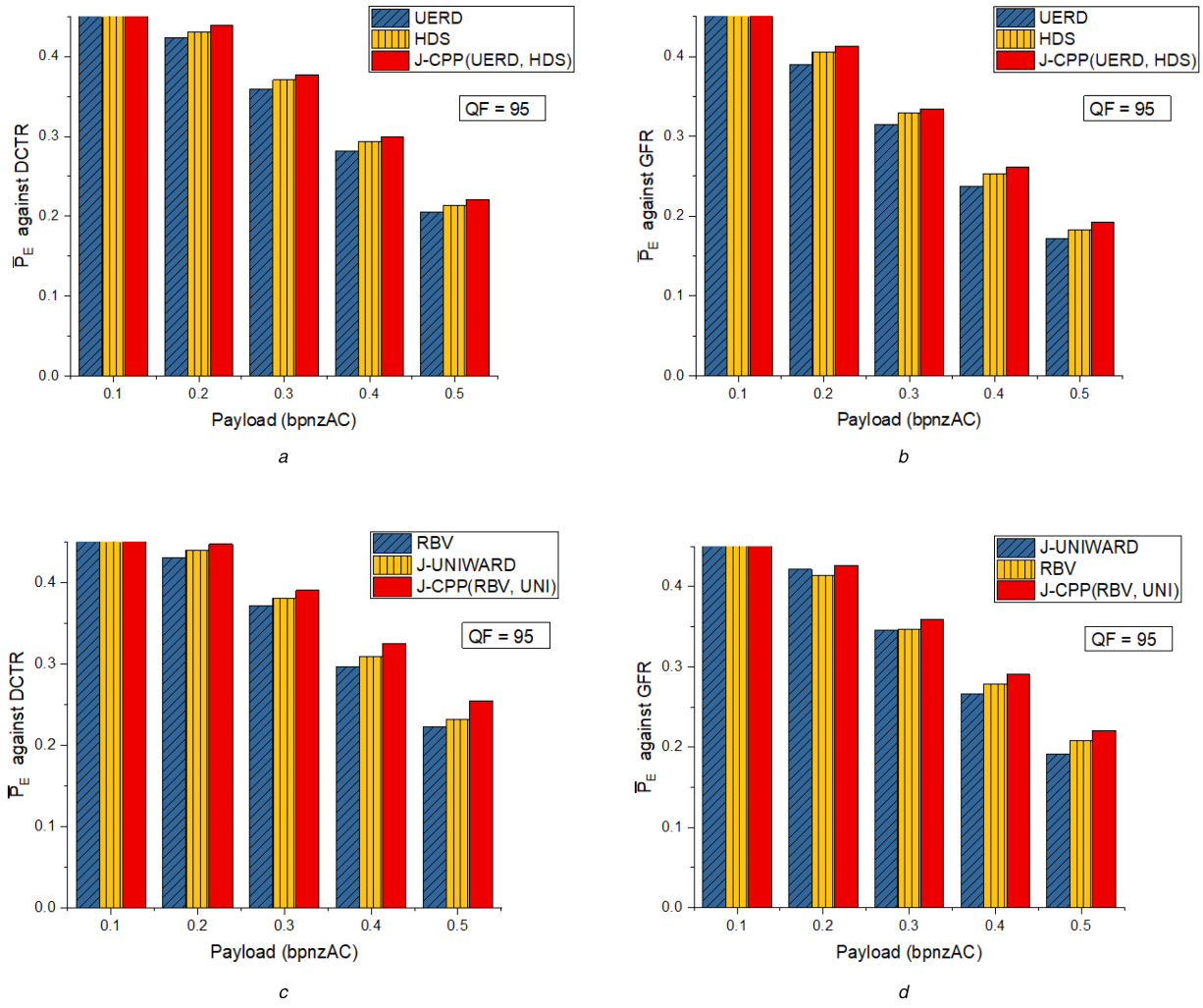

Fig. 7 *Testing errors under the detection of two steganalysis features with QF = 95*
(a) UERD, HDS and J-CPP(UERD,HDS) against DCTR, ***(b)*** UERD, HDS and J-CPP (UERD, HDS) against GFR, ***(c)*** J-UNIWARD, RBV and J-CPP (RBV, UNI) against DCTR, ***(d)*** J-UNIWARD, RBV and J-CPP (RBV, UNI) against GFR

Table 5 Numerical values of testing error and standard deviation for Fig. 7

Feature	Embedding method	Testing errors from 0.1 to 0.5 bpnzAC				
		0.1	0.2	0.3	0.4	0.5
DCTR	UERD	0.4759 ± 0.0019	0.4241 ± 0.0020	0.3596 ± 0.0031	0.2812 ± 0.0017	0.2056 ± 0.0018
	HDS	0.4793 ± 0.0021	0.4307 ± 0.0030	0.3705 ± 0.0026	0.2937 ± 0.0024	0.2139 ± 0.0022
	J-CPP(UERD,HDS)	0.4836 ± 0.0025	0.4388 ± 0.0020	0.3773 ± 0.0014	0.2998 ± 0.0018	0.2211 ± 0.0014
	promotion, %	0.43	**0.81**	**0.68**	**0.61**	**0.72**
	RBV	0.4759 ± 0.0020	0.4307 ± 0.0031	0.3720 ± 0.0019	0.2967 ± 0.0023	0.2224 ± 0.0032
	J-UNIWARD	0.4815 ± 0.0019	0.4402 ± 0.0024	0.3809 ± 0.0023	0.3094 ± 0.0025	0.2314 ± 0.0018
	J-CPP(RBV,UNI)	0.4860 ± 0.0022	0.4475 ± 0.0012	0.3907 ± 0.0021	0.3252 ± 0.0025	0.2544 ± 0.0017
	promotion, %	0.45	**0.73**	**0.98**	**1.58**	**2.30**
GFR	UERD	0.4547 ± 0.0022	0.3899 ± 0.0024	0.3148 ± 0.0026	0.2375 ± 0.0015	0.1720 ± 0.0014
	HDS	0.4631 ± 0.0022	0.4061 ± 0.0022	0.3290 ± 0.0019	0.2531 ± 0.0021	0.1831 ± 0.0021
	J-CPP(UERD,HDS)	0.4662 ± 0.0016	0.4133 ± 0.0042	0.3342 ± 0.0018	0.2612 ± 0.0019	0.1919 ± 0.0017
	promotion, %	0.31	0.72	**0.52**	**0.81**	**0.88**
	RBV	0.4658 ± 0.0017	0.4135 ± 0.0018	0.3465 ± 0.0014	0.2786 ± 0.0020	0.2084 ± 0.0024
	J-UNIWARD	0.4737 ± 0.0021	0.4214 ± 0.0022	0.3458 ± 0.0028	0.2666 ± 0.0018	0.1913 ± 0.0023
	J-CPP(RBV,UNI)	0.4753 ± 0.0018	0.4263 ± 0.0027	0.3589 ± 0.0024	0.2914 ± 0.0020	0.2206 ± 0.0014
	promotion, %	0.16	0.48	**1.24**	**1.28**	**1.22**

Bold values indicate the statistical significance of the promotion.

9 References

[1] Fridrich, J.: '*Steganography in digital media: principles, algorithms and applications*' (Cambridge University Press, Cambridge, 2009)

[2] Pevný, T., Fridrich, J.: 'Benchmarking for steganography'. Proc. Tenth Int. Workshop Information Hiding, Sana Barbara, CA, USA, May 2008, pp. 251–267

[3] Sarreshtedari, S., Akhaee, M. A.: 'One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme', *IET Image Process.*, 2014, **8**, (2), pp. 78–89

[4] Ahani, S., Ghaemmaghami, S.: 'Colour image steganography method based on sparse representation', *IET Image Process.*, 2015, **9**, (6), pp. 496–505

[5] Girdhar, A., Kumar, V.: 'Comprehensive survey of 3D image steganography techniques', *IET Image Process.*, 2018, **12**, (1), pp. 1–10

[6] Filler, T., Judas, J., Fridrich, J.: 'Minimizing additive distortion in steganography using syndrome trellis codes', *IEEE Trans. Inf. Forensics Sec.*, 2010, **6**, (3), pp. 920–935

[7] Pevný, T., Filler, T., Bas, T.: 'Using high-dimensional image models to perform highly undetectable steganography'. Proc. 12th Int. Workshop Information Hiding, Calgary, AB, Canada, June 2010, pp. 161–177

[8] Pevný, T., Bas, T., Fridrich, J.: 'Steganalysis by subtractive pixel adjacency matrix', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (2), pp. 215–224

[9] Fridrich, J., Kodovský, J.: 'Rich models for steganalysis of digital images', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (3), pp. 868–882

[10] Holub, V., Fridrich, J.: 'Designing steganographic distortion using directional filters'. Proc. IEEE Workshop Information Forensic and Security, Costa Adeje – Tenerife, Spain, December, 2012, pp. 234–239

[11] Houlb, V, Fridrich, J.: 'Digital image steganography using universal distortion'. Proc. First ACM Workshop Information Hiding and Multimedia Security, Montpellier, France, June 2013, pp. 59–68

[12] Li, B., Wang, M., Huang, J.W., *et al.*: 'A new cost function for spatial image steganography'. Proc. IEEE Int. Conf. Image Processing, Paris, France, October 2014, pp. 4206–4210

[13] Holub, V., Fridrich, J., Denemark, T.: 'Universal distortion function for steganography in an arbitrary domain', *EURASIP J. Inf. Sec.*, 2014, **1**, pp. 1–13

[14] Guo, L.J., Ni, J.Q., Shi, Y.Q.: 'Uniform embedding for efficient JPEG steganography', *IEEE Trans. Inf. Forensics Sec.*, 2014, **9**, (5), pp. 814–825

[15] Guo, L.J., Ni, J.Q., Su, W.K., *et al.*: 'Using statistical image model for JPEG steganography: uniform embedding revisited', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (12), pp. 2669–2680

[16] Wang, Z.C., Zhang, X.P., Yin, Z.X.: 'Hybrid distortion function for JPEG steganography', *J. Electron. Imaging*, 2016, **25**, (5), p. 050501

[17] Wei, Q., Yin, Z.X., Wang, Z.C., *et al.*: 'Distortion function based on residual blocks for JPEG steganography', *Multimedia Tools Appl.*, 2017, **25**, (5), pp. 1–14

[18] Zhou, W.B., Zhang, W.M., Yu, N.H.: 'A new rule for cost reassignment in adaptive steganography', *IEEE Trans. Inf. Forensic Sec.*, 2017, **12**, (11), pp. 2654–2667

[19] Zhou, W.B., Zhang, W.M., Yu, N.H.: 'Evolving distortion function by exploiting the differences among comparable adaptive steganography'. Proc. 12th Int. Conf. Natural Computation, Fuzzy Systems and Knowledge Discovery, Changsha, China, August 2016, pp. 1235–1244

[20] Filler, T., Fridrich, J.: 'Gibbs construction in steganography', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (4), pp. 705–720

[21] Li, B., Tan, S.Q., Wang, M., *et al.*: 'Investigation on cost assignment in spatial image steganography', *IEEE Trans. Inf. Forensics Sec.*, 2014, **9**, (8), pp. 1264–1277

[22] Bas, P., Filler, T., Pevný, T.: 'Break our steganographic system – the ins and outs of organizing boss'. Proc. 13th Int. Workshop Information Hiding,, Prague, Czech Republic, May 2011, pp. 59–70

[23] Holub, V., Fridrich, J.: 'Low-complexity features for JPEG steganalysis using undecimated DCT', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (2), pp. 219–228

[24] Bas, P., Furon, T.: 'BOWS-2 contest (break our watermarking system)', Organised within the activity of the Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT, 2008

[25] Fridrich, J., Filler, T.: 'Practical methods for minimizing embedding impact in steganography'. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, USA, February 2007, p. 650502

[26] Song, X.F., Liu, F.L., Yang, C.F., *et al.*: 'Steganalysis of adaptive JPEG steganography using 2D gabor filters'. Proc. Third ACM Workshop Inf. Hiding and Multimedia Security, Portland, OR, USA, June 2015, pp. 15–23

[27] Kodovský, J., Fridrich, J., Holub, V.: 'Ensemble classifiers for steganalysis of digital media', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (2), pp. 432–444